Правительство Российской Федерации

Федеральное государственное автономное образовательное

учреждение высшего образования   
"Национальный исследовательский университет   
"Высшая школа экономики"

Московский институт электроники и математики им. А. Н. Тихонова

Департамент прикладной математики

ОТЧЕТ

по курсовой работе по дисциплине

«Основы информационной безопасности»

Выполнил студент гр. СКБ171

Астраханцев Роман Геннадьевич

Тема работы: **«Определение комплекса мер обеспечения защиты объекта информатизации от актуальных угроз безопасности информации»**

Москва, 2020 г.

Оглавление

[Аэропорт им. Егора Летова с источниками информации 1](#_Toc40332475)

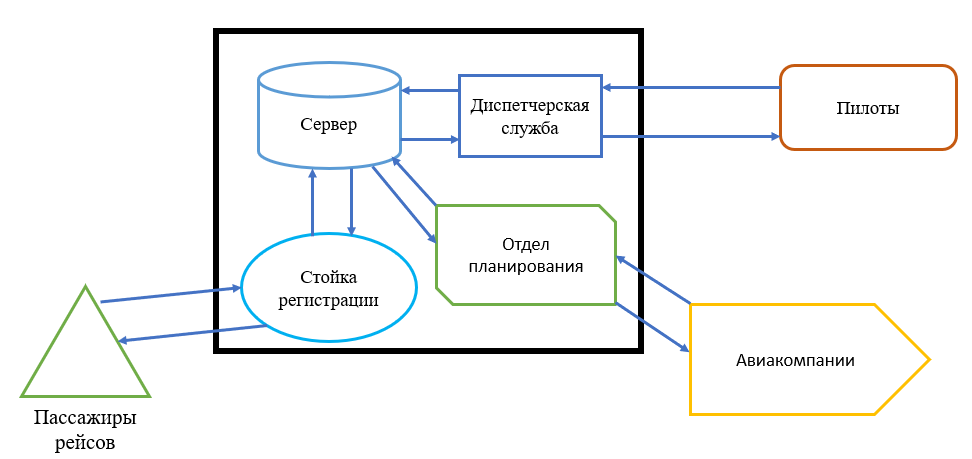
[Уточнение потоков информации 1](#_Toc40332476)

[Способы передачи информации 2](#_Toc40332477)

[Свойства информации, которые необходимо обеспечить 1](#_Toc40332478)

[Угрозы безопасности информации 2](#_Toc40332479)

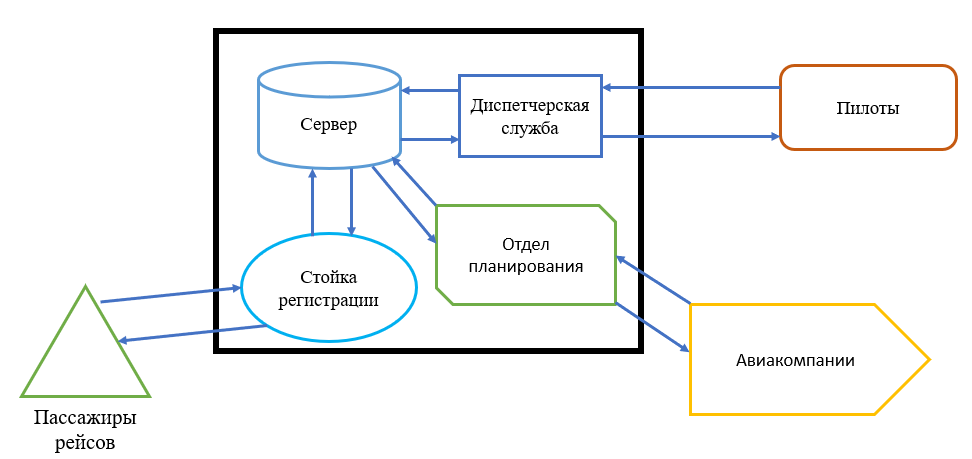
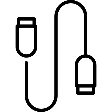
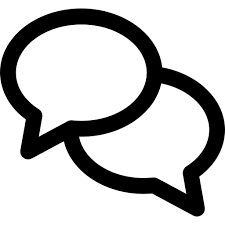
# **Аэропорт им. Егора Летова с источниками информации**



# **Уточнение потоков информации**

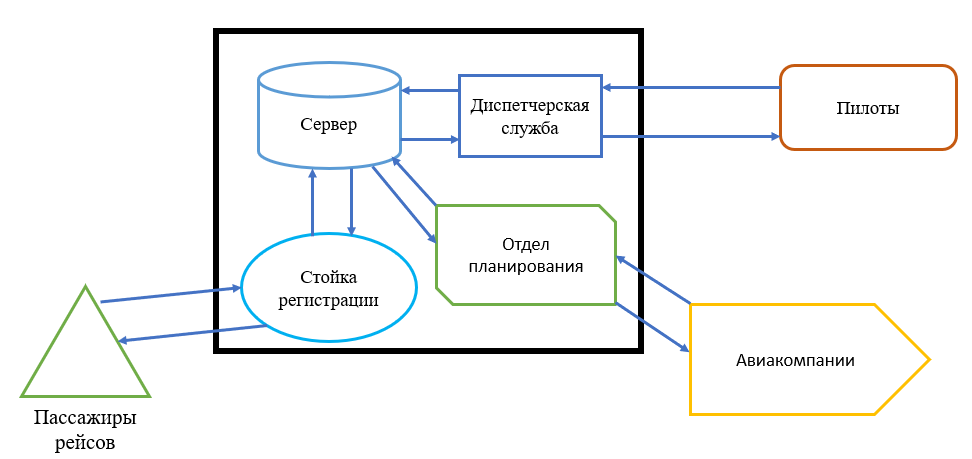
|  |  |
| --- | --- |
| **Поток** | **Дополнительная информация** |
| Пилот ⇒ Диспетчерская служба | Номер борта, полоса на которую заходишь и намерения (на стоянку, переждать, на заправку и т.д.) |
| Диспетчерская служба ⇒ Пилот | Вектор направления движения самолёта, разрешение на посадку |
| Сервер ⇒ Диспетчерская служба | Информация о наличии топлива, наличии свободной полосы, наличии парковочного места |
| Диспетчерская служба ⇒ Сервер | Запрашиваются на данные о наличии топлива, наличии свободной полосы, наличии парковочного места. Предаются регистрационные данные прилетевшего судна борта, факт прилёта/вылета. |
| Авиакомпания ⇒ Отдел планирования | Список рейсов на прилёт/отлёт, количество требуемых стояночных мест, количество требуемого топлива на даты соответствующих рейсов |
| Отдел планирования ⇒ Авиакомпания | Подтверждение получения информации, согласование возможности принятия рейсов на итоговую дату. |
| Отдел планирования ⇒ Сервер | Согласованные данные, полученные от авиакомпаний, затраты на покупку топлива. |
| Сервер ⇒ Отдел планирования | Количество топлива и посадочных мест для предоставления прилетающим бортам |
| Пассажиры рейсов ⇒ Стойка регистрации | Данные о брони, паспортные данные, информация о багаже |
| Стойка регистрации ⇒ Пассажиры рейсов | Посадочный талон |
| Стойка регистрации ⇒ Сервер | Запрос на наличие брони. Факт прибытия пассажира, информацию о багаже этого пассажира. |
| Сервер ⇒ Стойка регистрации | Талон на посадку для конкретного пассажира |

# **Способы передачи информации**



|  |  |  |  |
| --- | --- | --- | --- |
| Возникновение и распространение Радиоволн. | Кабель | Бесплатно значок | Листы бумаги значок векторное изображение | Векторы общественного ... | диалог, воздушный шар бесплатно значок из Outicons |
| **Радиоэфир** | **Электронный файл** | **Бумажный носитель** | **Посредством диалога** |

# **Свойства информации, которые необходимо обеспечить**



**Ц**

**К**

**К**

**Ц, Д, К**

**Ц, К**

**Ц, Д**

**Ц**

**Ц, К**

**Ц, Д**

**Ц**

**Ц, К**

**Ц**Ф

**Ц – Целостность, К – Конфиденциальность, Д - Доступность**

# **Угрозы безопасности информации**

УИБ1 = [террорист; открытость радиоэфира; включение устройства, нарушающего радиоэфир; радиоэфир; отсутствие возможности передачи информации по радиоэфиру (отсутствие связи между диспетчером и пилотом)];

(Свойство целостности: Пилот ⇒ Диспетчерская служба, Диспетчерская служба ⇒ Пилот)

УИБ2 = [хакерская группировка; отсутствие отдельной сети для работы сервера; внедрение вредоносного ПО; сервер аэропорта; кража данных на сервере];

(Свойство конфиденциальности: Отдел планирования ⇒ Сервер, Стойка рестрикции ⇒ Сервер, Сервер ⇒ Стойка регистрации)

УИБ3 = [уборщица; отсутствие регламента действий; затопление сервера; ведро с водой, комната с сервером; вывод сервера из строя];

(Свойство доступности: Сервер ⇒ Стойка отдел планирования, Сервер ⇒ Диспетчерская служба, Сервер ⇒ Стойка регистрации)

УИБ4 = [бывший администратор ИС; отсутствие регламента по смене пароля на сервере; проникновение на сервер и внедрение паразитических вирусов; сервер; изменение персональных данных и служебной информации];

(Свойство целостности: Сервер ⇒ Стойка отдел планирования, Сервер ⇒ Диспетчерская служба, Сервер ⇒ Стойка регистрации, Стойка отдел планирования ⇒ Сервер, Диспетчерская служба ⇒ Сервер, Стойка регистрации ⇒ Сервер)

УИБ5 = [сотрудник на стойке регистрации; отсутствие проверки сотрудника; найм злоумышленника на работу; стойка регистрации; кража персональных данных пассажиров];

(Свойство конфиденциальности: Стойка регистрации ⇒ Пассажиры рейсов, Пассажиры рейсов ⇒ Стойка регистрации)

УИБ6 = [авиакомпания-злоумышленник; отсутствие антивирусной программы; email-рассылка с вредоносными программами; ПК отдела планирования; кража данных других авиакомпаний о запланированных рейсах];

(Свойство конфиденциальности: Авиакомпании ⇒ Отдел планирования)

УИБ7 = [авиакомпания-злоумышленник; отсутствие проверки сотрудника; найм подставного сотрудника на работу; отдел планирования; контроль документов сообщения между авиакомпаниями и отделом планирования];

(Свойство целостности: Авиакомпании ⇒ Отдел планирования, Отдел планирования ⇒ Авиакомпании)

УИБ8 = [разработчик ПО; отсутствие системы тестирования ПО; ошибка в коде программы повлекшая некорректный ответ за запрос; диспетчер; нарушение корректной работы авиасообщения аэропорта (с потенциальным столкновением двух самолётов)]

(Свойство целостности: Сервер ⇒ Диспетчерская служба)

УИБ9 = [ураган; отсутствие дополнительного источника питания; поломка на электростанции; внутренняя система электропитания аэропорта; отключение электричества]

(Свойство доступности: Сервер ⇒ Стойка отдел планирования, Сервер ⇒ Диспетчерская служба, Сервер ⇒ Стойка регистрации)

(Свойство целостности: Сервер ⇒ Стойка отдел планирования, Сервер ⇒ Диспетчерская служба, Сервер ⇒ Стойка регистрации, Стойка отдел планирования ⇒ Сервер, Диспетчерская служба ⇒ Сервер, Стойка регистрации ⇒ Сервер)

(Свойство целостности: Пилот ⇒ Диспетчерская служба, Диспетчерская служба ⇒ Пилот)

УИБ10 = [подставной курьер; отсутствие проверки документов курьера; передача посылки злоумышленнику; ответный документ от аэропорта к авиакомпании; изменение ответного сообщения];

(Свойство целостности: Отдел планирования ⇒ Авиакомпании)

# **Модели нарушителей**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Нарушитель** | **Тип** | **Вид** | **Потенциал** | **Цели** | **Способы реализации** |
| Подставной курьер | Внешний | Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора | Базовый (? Базовый повышенный) | Получение конкурентных преимуществ | Воздействие на пользователей, администраторов безопасности, администраторов  информационной системы или обслуживающий персонал |
| Авиакомпания-злоумышленник | Внешний | Пользователи ИС | Базовый (? Базовый повышенный) | Получение конкурентных преимуществ | Несанкционированный доступ и (или) воздействие на объекты на прикладном уровне |
| Подставной сотрудник на стройке регистрации | Внутренний | Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора | Базовый | Причинение имущественного ущерба путем мошенничества или иным преступным путем | Воздействие на пользователей, администраторов безопасности, администраторов  информационной системы или обслуживающий персонал |
| Подставной сотрудник в отделе планирования | Внутренний | Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора | Базовый (? Базовый повышенный) | Получение конкурентных преимуществ | Воздействие на пользователей, администраторов безопасности, администраторов  информационной системы или обслуживающий персонал |
| Разработчик ПО | Внутренний | Разработчики, производители, поставщики программных, технических и программнотехнических средств | Базовый повышенный | Реализация угроз безопасности информации непреднамеренно из-за неосторожности или неквалифицированных действий | Несанкционированный доступ и (или) воздействие на объекты на аппаратном уровне |
| Террорист, мешающий радиоэфиру | Внешний | Террористические, экстремистские группировки | Базовый повышенный | Организация террористического акта | Несанкционированный физический доступ и (или) воздействие на линии (каналы) связи,  технические средства, машинные носители информации |
| Администратор ИС | Внутренний | Администраторы информационной системы и администраторы безопасности; Бывший сотрудник | Базовый повышенный (? Базовый) | Реализация угроз безопасности информации из мести | Несанкционированной доступ и (или) воздействие на объекты на общесистемном уровне |
| Уборщица | Внутренний | Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора | Базовый | Реализация угроз безопасности информации непреднамеренно из-за неосторожности или неквалифицированных действий | Несанкционированный физический доступ и (или) воздействие на линии (каналы) связи,  технические средства, машинные носители информации |
| Хакерская группировка | Внешний | Преступные группы | Базовый повышенный | Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды | Несанкционированный доступ и (или) воздействие на объекты на сетевом уровне |

# **Уровень проектной защищенности**